Configuração de sistemas de detecção de intrusão e prevenção de ataques

1- **Firewall Avançado**: Implementar firewalls de próxima geração para monitorar e filtrar tráfego indesejado.

2- **Sistemas de Detecção e Prevenção de Intrusão (IDS/IPS)**: Utilizar sistemas que detectam e previnem atividades suspeitas e ataques.

3- **Treinamento de Conscientização**: Treinar regularmente os funcionários sobre práticas seguras de TI e ameaças de phishing.

4-**Autenticação Multi-fator (MFA)**: Adotar MFA para garantir que apenas usuários autorizados acessem os sistemas.

5- **Análise de Log**: Monitorar e analisar logs de sistema para identificar comportamentos anômalos.

6-**Atualizações Regulares**: Manter todos os softwares e sistemas operacionais atualizados com os patches de segurança mais recentes.

7-**Criptografia**: Implementar criptografia para dados em trânsito e em repouso para proteger informações sensíveis.

8-**Segmentação de Rede**: Dividir a rede em segmentos menores para limitar o movimento lateral de invasores.

9-**Simulações de Ataques (Pen Testing)**: Realizar testes de penetração regulares para identificar e corrigir vulnerabilidades.

10-**Políticas de Acesso**: Estabelecer políticas rígidas de controle de acesso baseadas no princípio de privilégio mínimo.